Dans tout le problème V désigne un espace vectoriel euclidien de dimension 3, $O(V)$ le groupe orthogonal de V, c'est-à-dire le groupe des isométries (sous-entendu vectorielles) de V et $O^+(V)$ le groupe des isométries positives, c'est-à-dire des rotations (sous-entendu vectorielles) de V.
La sphère unité de V est notée S. Si r est une rotation distincte de Id_V, l'axe de r est une droite vectorielle qui coupe S en deux points opposés qui seront appelés les **pôles** de r.
Le cardinal d'un ensemble X sera noté $|X|$.
Si H est un sous-groupe d'un groupe G et si $a \in G$ on rappelle qu'on pose :

$$aH = \{\, g \in G \mid \exists\, h \in H, \quad g = ah \,\}.$$

L'application $h \mapsto ah$ est alors une bijection de H sur aH.

0. Questions préliminaires.

0.1 Soit $\mathbf{U}$ le groupe (multiplicatif) des nombres complexes de module 1 et soit G un sous-groupe fini de cardinal n de $\mathbf{U}$. Montrer que G est un groupe cyclique. (On pourra comparer G et le groupe $\mathbf{U}_n$ des racines n-ièmes de l'unité.)

0.2 Soit X un ensemble fini et soit $f : X \to Y$ une application. Montrer qu'on a la formule suivante (dite lemme de comptage) : $|X| = \sum_{y \in Y} |f^{-1}(\{y\})|$.

I. Première partie.

Dans cette partie, G désigne un sous-groupe fini de $O^+(V)$ et n son cardinal. On suppose $n > 1$ et on note P l'ensemble des pôles des éléments de G distincts de Id_V.

I.1 Soit $r \in G$ et x un pôle de r. Soit $g \in G$. Montrer que $g(x)$ est pôle d'un élément de G que l'on précisera.

En vertu de I.1, le groupe G opère sur l'ensemble P par $g.x = g(x)$. Soit $x \in P$. On note ω_x l'orbite de x sous l'action de G, c'est-à-dire l'ensemble des $g.x$ pour $g \in G$ et H_x le stabilisateur de x, c'est-à-dire le sous-groupe des $g \in G$ tels que $g.x = x$ et on pose $v_x = |\omega_x|$ et $n_x = |H_x|$.

I.2 Soit $x \in P$ et Φ_x l'application de G dans ω_x définie par $\Phi_x(g) = g(x)$. Montrer que tous les ensembles $\Phi_x^{-1}(\{y\})$ pour $y \in \omega_x$ sont en bijection avec H_x. En déduire la formule $n = v_x n_x$ (on pourra utiliser 0.2).

I.3 Soit $x \in P$. Montrer que H_x est un groupe cyclique de cardinal ≥ 2. Montrer que G est réunion des stabilisateurs H_x pour $x \in P$.

On désigne par E l'ensemble des couples (r, x) où r est un élément de G distinct de Id_V et x un pôle de r.

I.4 Montrer qu'on a $|E| = 2(n-1)$.

On suppose que le nombre d'orbites de G dans P est égal à k et on choisit un pôle dans chaque orbite : $x_1, \cdots, x_k$. On pose $\omega_i = \omega_{x_i}$, $v_i = v_{x_i}$ et $n_i = n_{x_i}$. On a donc $n_i \geq 2$.

I.5 Montrer la formule :

$$|E| = \sum_{i=1}^{k} v_i(n_i - 1).$$

I.6 Montrer que l'on a :

$$2 - \frac{2}{n} = \sum_{i=1}^{k} \left(1 - \frac{1}{n_i}\right). \tag{1}$$

I.7 Montrer que les seules valeurs possibles de k sont 2 et 3.

I.8 On suppose $k = 2$. Montrer que G est un groupe cyclique. Donner un exemple d'un tel sous-groupe de $O^+(V)$ de cardinal $n \in \mathbf{N}^*$ donné.

Dans tout le reste de la première partie on suppose $k = 3$ et, pour fixer les notations, $n_1 \leq n_2 \leq n_3$.

I.9 Montrer qu'on a les résultats suivants :
a) $n_1 = 2$.
b) $n_2 \in \{2, 3\}$.
c) si $n_2 = 3$, alors $n_3 \in \{3, 4, 5\}$.

I.10 On suppose qu'on a $n_1 = n_2 = 2 \leq n_3$ et on pose $n_3 = m$. Déterminer le cardinal de G en fonction de m. Montrer que G contient un sous-groupe distingué H qui est cyclique de cardinal m. Montrer que les éléments de $G - H$ sont d'ordre 2.
Donner un exemple d'un tel sous-groupe G de $O^+(V)$ pour $m \geq 2$ donné.

I.11 On suppose qu'on a $n_1 = 2$, $n_2 = 3$ et $n_3 = 3, 4$ ou 5. Déterminer selon les cas la valeur de $|G|$. Déterminer selon les cas étudiés ci-dessus les ordres possibles des éléments de G et préciser le nombre d'éléments de chaque ordre.

II. Deuxième partie.

Dans cette partie G désigne un sous-groupe de $O(V)$. On pose $G^+ = G \cap O^+(V)$ et $G^- = G - G^+$ et on suppose $G^+ \neq G$. On note $-\mathrm{Id}_V$ l'homothétie de rapport -1 dans V et, pour $u \in O(V)$, on pose $-u = -\mathrm{Id}_V \circ u$. Si A est une partie de $O(V)$, $-A$ désigne l'ensemble des $-u$, pour $u \in A$.

II.1 Montrer que G^+ est un sous-groupe distingué de G et déterminer le groupe quotient. Montrer que si s est dans G^- on a $G^- = sG^+$ et que s^2 est dans G^+. L'ensemble G^- est-il un sous-groupe de G ?

II.2 Soient A et B deux groupes. On munit le produit $A \times B$ de la loi de composition définie par $(a, b)(a', b') = (aa', bb')$. Montrer que $A \times B$, muni de cette loi, est un groupe. On désigne ce groupe comme le produit direct de A et B.

II.3 On suppose $-\mathrm{Id}_V \in G$. Montrer que G est isomorphe au produit direct $G^+ \times \{1, -1\}$.

II.4 Montrer que $\widehat{G} = G^+ \cup (-G^-)$ est un sous-groupe de $O^+(V)$.
On suppose $-\mathrm{Id}_V \notin G$. Montrer que G est isomorphe à $\widehat{G}$.

II.5 Comment peut-on décrire, à isomorphisme près, les sous-groupes finis de $O(V)$ lorsqu'on connaît ceux de $O^+(V)$?

III. Troisième partie.

On note τ le nombre d'or $\tau = \dfrac{1+\sqrt{5}}{2} \sim 1,618$. On rappelle les formules : $\tau^2 = \tau+1$ et $\tau^{-1} = \tau - 1$.

Dans cette partie, l'espace V est l'espace $\mathbf{R}^3$ muni du produit scalaire usuel pour lequel la base canonique $e_1 = (1,0,0)$, $e_2 = (0,1,0)$, $e_3 = (0,0,1)$ est orthonormée. On note O l'origine, $O = (0,0,0)$.
On considère l'ensemble D formé des 20 points ci-dessous (le signe $\pm$ prend toutes les valeurs possibles) :

$$D = \{\ (\pm 1, \pm 1, \pm 1)\ ;\ (0 \pm \tau^{-1}, \pm\tau)\ ;\ (\pm\tau, 0, \pm\tau^{-1})\ ;\ (\pm\tau^{-1}, \pm\tau, 0)\ \}$$

On désigne par G le sous-groupe de $O(V)$ formé des éléments g qui laissent invariant D , c'est-à-dire vérifient $g(D) = D$. On reprend les notations G^+ et G^- comme dans la deuxième partie.

III.1 Montrer que les points de D sont sur une même sphère de centre l'origine. Déterminer l'isobarycentre des points de D. Déterminer les isométries affines qui conservent D.

Soit σ une permutation **paire** de l'ensemble $\{1,2,3\}$ et soit $\epsilon = (\epsilon_1, \epsilon_2, \epsilon_3)$ un élément de $\{1,-1\}^3$. On considère la transformation $u_{\sigma,\epsilon}$ définie par la formule

$$u_{\sigma,\epsilon}(e_i) = \epsilon_i e_{\sigma(i)} \qquad \text{pour} \quad i = 1,2,3.$$

Soit H l'ensemble des transformations $u_{\sigma,\epsilon}$ pour $\sigma \in \mathcal{A}_3$ et $\epsilon \in \{1,-1\}^3$.

III.2 Montrer que H est contenu dans $O(V)$, déterminer $|H|$ et $H^+ = H \cap O^+(V)$. Montrer qu'on a $H \simeq H^+ \times \{1,-1\}$ (cf. II.2 et II.3). Montrer que H est contenu dans G, de sorte que H opère sur D. Montrer que H admet sur D deux orbites que l'on précisera.

III.3 On pose $a = (1,1,1)$, $b = (0, \tau^{-1}, \tau)$, $m = (\tau^{-1}, 1, \tau)$. On considère le demi-tour d'axe Om, que l'on note v_m. Montrer que l'on a $v_m(a) = b$, puis que v_m est dans G.

III.4 Déduire de III.3 que G opère transitivement sur D. Montrer que $|G|$ est multiple de 20 (cf. I.2) et de 24, donc de 120.

III.5 Montrer que G^+ opère transitivement sur D.

III.6 On reprend les notations de III.3 et on pose, de surcroît, $c = (\tau, 0, \tau^{-1})$ et $d = (\tau^{-1}, \tau, 0)$.

a) Soit $g \in G$. On suppose que g laisse fixe b, c, d. Montrer que g est l'identité.

b) Soit G_a le stabilisateur de a. Montrer que G_a permute les points b, c, d (on pourra considérer la position des points de D par rapport au plan d'équation $x + y + z = \sqrt{5}$).

c) Montrer qu'on a $|G_a| \leq 6$ et en déduire qu'on a $|G| = 120$.

III.7 Déterminer les ordres des éléments de G (utiliser les résultats de I).